《信息隐藏技术》课程Project

2023-推荐参考文献清单

**一、领域相关的高质量会议期刊**

1. 会议
   1. 信息安全顶会：UseNix，S&P，CCS， NDSS
   2. 机器学习：NIPS，ILCR，ICML，AAAI
   3. 自然语言处理NLP：ACL
   4. 视频：CVPR，ICCV，ECCV
   5. 信息隐藏： IH&MMSEC，IWDW
   6. 音频：ICASSP, Interspeech
2. 期刊
   1. 信息安全：TIFS
   2. 信号处理：TPAMI，TASSP，TMM，TSP （IEEE Transaction on…）

**二、相关资源获取**

1. **学术专用搜索网站**
   1. <https://scholar.google.com/>
   2. [https://dblp.org](https://dblp.org/)
   3. <https://www.semanticscholar.org/>
   4. <https://academic.microsoft.com/>
   5. <https://www.aminer.org/>
2. **下载文献平台**
   1. [https://sci-hub.tw/](https://tool.yovisun.com/scihub/)
   2. <https://tool.yovisun.com/scihub/>
   3. <http://www.sci-hub.ac.cn/>
3. **获取代码**
   1. **作者个人主页**
   2. **PapersWithCode,** <https://paperswithcode.com/>
   3. **代码托管平台**
      1. **GitHub,** <https://github.com/>
      2. **SourceForge,** <https://sourceforge.net/>
      3. **码云，** <https://gitee.com/>
   4. **向作者发邮件索要**
4. **信息隐藏相关资源**
   1. **Jiessia fridrich 网站**
   2. **微信公众号：隐者联盟**

**三、参考论文清单**

注意：本清单文献仅供大家**参考**。Project的工作内容并不受该清单内容的限制。大部分文献是近3年内（2021-2023）在信息隐藏和数字水印领域中的一些比较权威的新的工作，旨在扩展大家的认知范围。由于目前深度学习技术研究广泛，所以，本清单中的大部分工作与深度学习技术的使用和深度学习本身的保护相关，但是大家的Project并不要求一定要用深度学习技术，采用传统的方法，有自己对问题的思考，分析和解决都是可以的。Project不以结果确定成绩，而是以你们自己对问题的分析和探索，以及解决问题的整个过程作为评价，目标是让大家提升考虑实际问题，解决实际问题的能力。

1. 信息隐藏技术最新综述
   1. 张卫明, 王宏霞, 李斌, 任延珍, 杨忠良, 陈可江, 俞能海. (2022). 多媒体隐写研究进展. *中国图象图形学报*, *24*(6), 1918-1943.（CSIG 年度报告 2022，全面系统且新鲜，推荐阅读，总览该领域技术发展的全貌）
   2. Byrnes O, La W, Wang H, et al. Data Hiding with Deep Learning: A Survey Unifying Digital Watermarking and Steganography[J]. arXiv preprint arXiv:2107.09287, 2021(基于深度神经网络的信息隐藏和水印技术综述，总结得很好，可比较系统地了解该领域的代表性工作和技术发展脉络，35页)
   3. Muralidharan T, Cohen A, Cohen A, et al. The infinite race between steganography and steganalysis in images[J]. Signal Processing, 2022: 108711. （SP 2022，关于信息隐藏技术和隐写分析技术的互相对抗发展综述，55页，想全面深入了解信息隐藏技术发展脉络可以看看，其中的图很系统，方便大家了解现状）
2. 基于深度生成网络的隐写技术
3. 王健, 陈可江, 张卫明, 等. 面向可逆图像处理网络的可证安全自然隐写[J]. 2023.（很好，中文，可快速了解目前领域最新技术点）
4. Ding J, Chen K, Wang Y, et al. Discop: Provably Secure Steganography in Practice Based on “Distribution Copies”[C]//2023 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2023: 2238-2255.（S&P 信息安全四大顶会之一，可证明安全隐写的重要文献）
5. [StegaDDPM: Generative Image Steganography based on Denoising Diffusion Probabilistic Model](https://dl.acm.org/doi/abs/10.1145/3581783.3612514), 2023 ACM MM

（文章链接：https://dl.acm.org/doi/abs/10.1145/3581783.3612514）

1. Zhou Z, Dong X, Meng R, et al. Generative Steganography via Auto-Generation of Semantic Object Contours[J]. IEEE Transactions on Information Forensics and Security, 2023.
2. Chen K, Zhou H, Wang Y, et al. Cover Reproducible Steganography via Deep Generative Models[J]. IEEE Transactions on Dependable and Secure Computing, 2022.(TDSC 2022 通过深度生成模型进行载体重建)
3. Xu Y, Mou C, Hu Y, et al. Robust Invertible Image Steganography[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 7875-7884 （CVPR 2022， 鲁棒可逆图像隐写）
4. Wei P, Li S, Zhang X, et al. Generative Steganography Network[C]//Proceedings of the 30th ACM International Conference on Multimedia. 2022: 1621-1629.（ACM MM 生成隐写网络，将秘密消息映射成图片，隐藏信息，比较新颖）
5. 鲁棒隐写（利用社交软件进行隐蔽通信具有很好的应用价值，但是其面临着社交软件对图像的重压缩操作会破坏隐写数据的问题，因此，针对该类隐蔽通信通道而研究具备特定鲁棒性的大容量隐写算法，具有一定的实用价值）
6. Bui T, Agarwal S, Yu N, et al. RoSteALS: Robust Steganography using Autoencoder Latent Space[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2023: 933-942.
7. Fang H, Qiu Y, Chen K, et al. Flow-based robust watermarking with invertible noise layer for black-box distortions[C]//Proceedings of the AAAI conference on artificial intelligence. 2023, 37(4): 5054-5061.
8. Zeng K, Chen K, Zhang W, et al. Improving robust adaptive steganography via minimizing channel errors[J]. Signal Processing, 2022, 195: 108498.（SP 2022， 可以在facebook环境中使用的鲁棒隐写技术）
9. Liu Z, Yi X, Zhao X, et al. Content-Aware Robust JPEG Steganography for Lossy Channels Using LPCNet[J]. IEEE Signal Processing Letters, 2022, 29: 2253-2257.
10. You Z, Ying Q, Li S, et al. Image Generation Network for Covert Transmission in Online Social Network[C]//Proceedings of the 30th ACM International Conference on Multimedia. 2022: 2834-2842. (ACM MM 2022 ACM MM 2022， 图像生成技术，可以适用于社交网络（OSN）)
11. 抗摄屏水印（属于鲁棒水印技术，抗物理噪声攻击，具有很好的实用价值，是目前的研究热点）
12. Han Fang, Zhaoyang Jia, Zehua Ma, Ee-Chien Chang, and Weiming Zhang. PIMoG: An effective screen-shooting noiselayer simulation for deep-learning-based watermarking network. In MM ’22: The 30th ACM International Conference on Multimedia, Lisboa, Portugal, October 10 - 14, 2022,pages 2267–2275. ACM, 2022.（ACM MM 抗摄屏水印的新工作）
13. Fang H, Chen D, Wang F, et al. TERA: Screen-to-Camera Image Code with Transparency, Efficiency, Robustness and Adaptability[J]. IEEE Transactions on Multimedia, 2021, 24: 955-967（MM，2021， 抗摄屏水印，目前很受关注的工作，具有很好的实用价值）
14. Fang H, Zhang W, Ma Z, et al. A camera shooting resilient watermarking scheme for underpainting documents[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2019, 30(11): 4075-4089.
15. Fang H, Zhang W, Zhou H, et al. Screen-shooting resilient watermarking[J]. IEEE Transactions on Information Forensics and Security, 2018, 14(6): 1403-1418. （第一篇）
16. 音频隐写及水印
17. Zhang G, Zheng L, Su Z, et al. M-sequences and sliding window based audio watermarking robust against large-scale cropping attacks[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 1182-1195.(基于DWT-SVD + SS的鲁棒音频水印)
18. Ren Y, Zhu H, Zhai L, et al. Who is Speaking Actually? Robust and Versatile Speaker Traceability for Voice Conversion[J]. arXiv preprint arXiv:2305.05152, 2023.(ACM MM 2023， 基于VAE-FLOw的深度神经网络鲁棒音频隐写)
19. 文本隐写及水印
20. Wang H, Yang Z, Yang J, et al. Hi-Stega: A Hierarchical Linguistic Steganography Framework Combining Retrieval and Generation[C]//International Conference on Neural Information Processing. Singapore: Springer Nature Singapore, 2023: 41-54.（NIPs 2023 最新的文本隐写工作，建议大家关注）
21. Xiang L, Wang R, Yang Z, et al. Generative Linguistic Steganography: A Comprehensive Review[J]. KSII Transactions on Internet & Information Systems, 2022, 16(3). (生成式文本隐写综述)
22. Yang X, Chen K, Zhang W, et al. Watermarking Text Generated by Black-Box Language Models[J]. arXiv preprint arXiv:2305.08883, 2023.（文本水印新工作）
23. Yang X, Zhang W, Fang H, et al. Language universal font watermarking with multiple cross-media robustness[J]. Signal Processing, 2023, 203: 108791.（文本水印）
24. 神经网络模型水印（用于保护神经网络版权的水印，目前研究领域的新点）
25. 吴汉舟, 张杰, 李越, 等. 人工智能模型水印研究进展[J]. 中国图象图形学报, 2023, 28(6): 1792-1810. （综述性论文）
26. Lukas N, Jiang E, Li X, et al. Sok: How robust is image classification deep neural network watermarking?[C]//2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022: 787-804.(SP 2022，图像分类模型水印最新综述，论文讲解：https://mp.weixin.qq.com/s/ureKEsnnEC4RHHUEOKFmiw)
27. Yang P, Lao Y, Li P. Robust watermarking for deep neural networks via bi-level optimization[C]//Proceedings of the IEEE/CVF International Conference on Computer Vision. 2021: 14841-14850.
28. 安全隐写编码及损失函数设计（基于最小失真安全隐写框架的更深入的失真函数设计，以及安全编码算法相关工作）
    1. Guan Q, Liu P, Zhang W, et al. Double-Layered Dual-Syndrome Trellis Codes Utilizing Channel Knowledge for Robust Steganography[J]. IEEE Transactions on Information Forensics and Security, 2022, 18: 501-516.（利用通道信息的双层双STC编码，实现社交应用环境下的鲁棒隐写）
    2. Yao Q, Zhang W, Yu N. Optimality of Polar Codes in Additive Steganography under Constant Distortion Profile[C]//2022 14th International Conference on Wireless Communications and Signal Processing (WCSP). IEEE, 2022: 404-408.
29. 隐写分析
30. Zhao N, Chen K, Qin C, et al. Calibration-based Steganalysis for Neural Network Steganography[C]//Proceedings of the 2023 ACM Workshop on Information Hiding and Multimedia Security. 2023: 91-96.(IH &MMSEC 2023, 信息隐藏专业领域公认最重要会议)
31. Wang H, Yang Z, Yang J, et al. Linguistic Steganalysis in Few-Shot Scenario[J]. IEEE Transactions on Information Forensics and Security, 2023.（TIFS 2023 文本隐写分析）
32. Yang J, Yang Z, Zou J, et al. Linguistic Steganalysis Toward Social Network[J]. IEEE Transactions on Information Forensics and Security, 2022, 18: 859-871. （面向社交网络的文本隐写分析）
33. Guan Q, Chen K, Chen H, et al. Detecting Steganography in JPEG Images Recompressed with The Same Quantization Matrix[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022. (TCSVT 2022，JPEG 图像隐写分析)
34. Boroumand M, Chen M, Fridrich J. Deep residual network for steganalysis of digital images[J]. IEEE Transactions on Information Forensics and Security, 2018, 14(5): 1181-1193.（TIFS 2018，采用深度神经网络进行隐写分析的经典工作。）
35. 可逆信息隐藏（是信息隐藏研究领域中的一个新的分支，关注隐藏中Cover载体的无损恢复。目前，使用可逆隐写技术在加密图像中隐写成为一个新的热点话题，重要期刊会议出现多篇论文工作）
    1. Yao Y, Wang K, Chang Q, et al. Reversible Data Hiding in Encrypted Images Using Global Compression of Zero-valued High Bit-planes and Block Rearrangement[J]. IEEE Transactions on Multimedia, 2023.
    2. Chen K, Guan Q, Zhang W, et al. Reversible data hiding in encrypted images based on binary symmetric channel model and polar code[J]. IEEE Transactions on Dependable and Secure Computing, 2022. （TDSC 信息安全顶刊，加密图像中的可逆隐写）
    3. Li F, Qi Z, Zhang X, et al. JPEG reversible data hiding using dynamic distortion optimizing with frequency priority reassignment[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(12): 8849-8863.
    4. Yu M, Yao H, Qin C, et al. Reversible Data Hiding in Palette Images[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 33(2): 648-660.
    5. Weng S, Zhou Y, Zhang T, et al. General framework to reversible data hiding for JPEG images with multiple two-dimensional histograms[J]. IEEE Transactions on Multimedia, 2022.